Abstract

Private set intersection (PSI) is a two party protocol where both parties possess a private set and at the end of the protocol, one party (client) learns the intersection while other party (server) learns nothing. Motivated by some interesting practical applications, several *provably secure* and *efficient* PSI protocols have appeared in the literature in recent past. Some of the proposed solutions are secure in the honest-but-curious (HbC) model while the others are secure in the (stronger) malicious model. Security in the latter is traditionally achieved by following the classical approach of attaching a zero knowledge proof of knowledge (ZKPoK) (and/or using the so-called cut-and-choose technique). These approaches prevent the parties from deviating from normal protocol execution, albeit with significant computational overhead and increased complexity in the security argument, which includes in case of ZKPoK, knowledge extraction through rewinding.

We critically investigate a subset of the existing protocols. Our study reveals some interesting points about the so-called provable security guarantee of some of the proposed solutions. Surprisingly, we point out some gaps in the security argument of several protocols. We also discuss an attack on a protocol when executed multiple times between the same client and server. The attack, in fact, indicates some limitation in the existing security definition of PSI. On the positive side, we show how to correct the security argument for the above mentioned protocols and show that in the HbC model the security can be based on some standard computational assumption like RSA and Gap Diffie-Hellman problem. For a protocol, we give improved version of that protocol and prove security in the HbC model under standard computational assumption.

For the malicious model, we construct two PSI protocols using deterministic blind

signatures i.e., Boldyreva's blind signature and Chaum's blind signature, which do not involve ZKPoK or cut-and-choose technique. Chaum's blind signature gives a new protocol in the RSA setting and Boldyreva's blind signature gives protocol in gap Diffie-Hellman setting which is quite similar to an existing protocol but it is efficient and does not involve ZKPoK.